BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 4 :
G06F 13/14, 13/38, H04L 9/00
H04L 11/26

A1

(11) International Publication Number: WO 89/ 08887

(43) International Publication Date:
21 September 1989 (21.09.89)

(21) International Application Number: PCT/AU89/00098

(22) International Filing Date: 10 March 1989 (10.03.89)

(31) Priority Application Number: PI 7205

(32) Priority Date: 11 March 1988 (11.03.88)

(33) Priority Country: AU

(71) Applicant *(for all designated States except US)*: QPSX COMMUNICATIONS LTD. [AU/AU]; 33 Richardson Street, West Perth, W.A. 6005 (AU).

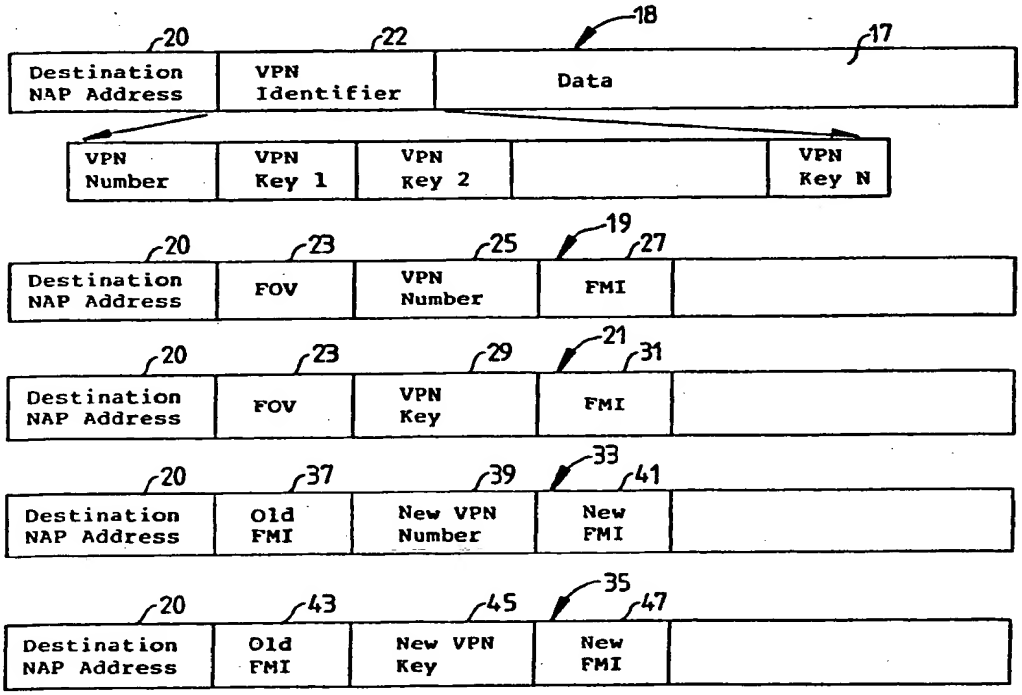
(72) Inventor; and
(75) Inventor/Applicant *(for US only)* : ALLES, Anthony, Lakshman [AU/AU]; Unit 10/152 Edinboro Street, Joondara, W.A. 6060 (AU).

(74) Agents: PRYOR, Geoffrey, C. et al.; Davies & Collison, 1 Little Collins Street, Melbourne, VIC 3000 (AU).

(81) Designated States: AT (European patent), AU, BE (European patent), CH (European patent), DE (European patent), FR (European patent), GB (European patent), IT (European patent), JP, LU (European patent), NL (European patent), SE (European patent), US.

Published
With international search report.

(54) Title: ACCESS SECURITY SYSTEM FOR SWITCHED COMMUNICATIONS NETWORKS



(57) Abstract

A method for securely transmitting signals in packets (18) between nodes (4) in a network (2), the method including the steps of providing in the packets security fields (22) which have first and second components, one of the components (VPN Number) being generated by the network administrator (6) and the second component (VPN Key) being generated by at least one of the nodes.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BG	Bulgaria
BJ	Benin
BR	Brazil
CF	Central African Republic
CG	Congo
CH	Switzerland
CM	Cameroon
DE	Germany, Federal Republic of
DK	Denmark
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
HU	Hungary
IT	Italy
JP	Japan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
LI	Liechtenstein
LK	Sri Lanka
LU	Luxembourg
MC	Monaco
MG	Madagascar
ML	Mali
MR	Mauritania
MW	Malawi
NL	Netherlands
NO	Norway
RO	Romania
SD	Sudan
SE	Sweden
SN	Senegal
SU	Soviet Union
TD	Chad
TG	Togo
US	United States of America

ACCESS SECURITY SYSTEM FOR SWITCHED COMMUNICATIONS NETWORKS

This invention relates to an access security system for switched communications networks.

The security system of the invention prevents unauthorized access to nodes attached or coupled to a switched communications network.

Normally it is not possible to access communications on the network other than through the nodes attached to the network. Typically a particular node is designated by one or more identifiers, Network Access Point Addresses (NAP Address), which uniquely identify the attachment point of that node throughout the network. An administrative entity is usually responsible for the allocation of NAP Addresses, and, for the purposes of this specification all entities responsible for the

administration of a network resource will be referred to by the generic title of "Network Administrator". The Network Administrator has the capability of communicating with nodes on the network through a particular node, referred to here as the "Network Administration Node".

A switched Communications Network is such as to enable any particular node, the "source node", N_s, attached to the network to engage in switched communication with any other node, the "destination node" N_d, attached to the network, where the only necessary requirement for communication to take place is the knowledge of a NAP Address of N_d by N_s. Examples of Switched Communications Networks include, but are not restricted to, packet switched networks, circuit switched networks and virtual circuit networks. Typically, communication between nodes is through the exchange of blocks of data, for instance, datagrams in packet switched networks and channels in virtual circuit networks..

Addressing and other control information is used to ensure that a communication from a node is received only by the intended destination node. Typically a source node prefixes at least the initial block of data with a NAP Address associated with the intended destination node and other control information. For instance, all datagrams in a packet switched network usually contain addressing and control information, whereas such information may be provided only during the connection phase in a circuit or virtual circuit switched network.

One known practice for the operation of such networks described above is for a node to accept all blocks prefixed with a NAP Address associated with that node. There is no need for prior authorization from either the destination node or the Network Administrator, before a source node initiates a communication with a destination node. This approach has the drawbacks that a node is neither able to verify the identity or authorization of the source node before accepting the message, nor is the node able to regulate the nodes with which it is willing to communicate. Thus, there is little security in such a system.

One proposal for partially overcoming these problems is for a destination node to regulate the nodes with which it is authorized to engage in communication, on the basis of the NAP Addresses of the source nodes. A source node appends a NAP Address corresponding to that node to at least the first data block transmitted to the destination node. Then each destination node checks the NAP Address of the source node upon the initiation of a communication, against a list of the NAP Addresses of the nodes from which the node is authorized to receive data. The received data block is accepted only if the source node's NAP Address is found in the list of authorized nodes. The list of authorized nodes is programmed either by the destination node or by the Network Administrator. This approach has the drawback, however, that the security checking is performed upon the source node's NAP Address. Since this is appended by the source node, its integrity cannot be guaranteed. Furthermore, since the NAP

Addresses are supplied by the Network Administrator, they are also subject to either accidental or unauthorized duplication or tampering by the Network Administrator.

Another proposal is for the system to arrange for the source node to check the destination node's NAP Address against a list of nodes to which the node is authorized to transmit data. Communication is initiated only if the destination node's NAP Address is found in the list. This approach suffers from similar problems to the technique discussed above, insofar as a destination node cannot have any guarantee that filtering has been performed and the NAP Addresses are subject to duplication or tampering by the Network Administrator.

Another known technique used to provide access security is to prefix at least the first data block of a communication with a "Security Field", which is checked against a pre-programmed field at the receiving node. Typically, the Security Field defines a security level or domain, either that from which the message originated or for which the message is intended. The message is received by a node only if the security level or domain of the message accords with that of the receiving node. This technique has the drawbacks that it requires such security levels or domains to be uniformly applicable throughout the network, which may not be appropriate in particular types of networks (for instance, public Networks) and it requires the Network Administrator to regulate the allocation of levels and domains and security Fields. Hence, the integrity of the scheme

is predicated upon the integrity of the Network Administrator. Examples of this technique are described in the following articles: M. St. Johns, "Draft Revised IP Security Option", RFC 1038, and L. Neitzel, "Proposal for an Optional Security LLC Sublayer", Proposal to IEEE 802.2.

The general object of the present invention is to overcome the drawbacks of the security techniques defined above.

According to the present invention there is provided a method of securely transmitting switched signals between nodes which are attached to a communications network, said communications network including a network administrator, said method including the steps of transmitting signals in blocks at least some of which include security fields, checking the security fields at the nodes and accepting the received signal at a node only if first and second components of the security field have a particular characteristic, and wherein the security field is established by generating the first component of the security field by the network administrator and generating the second component of the security field by at least one of the nodes.

The invention also provides a security system for a switched communications network which includes a network administrator and to which is attached a plurality of nodes, said system comprising means for transmitting signals between said nodes in signal blocks at least some of which include security fields, checking means at the nodes for checking the

security fields to determine whether or not the first and second components thereof have particular characteristics, and wherein said network administrator includes means for generating a first component of the security field and at least one of said nodes includes means for generating a second component of the security field.

In the method and system defined above, it will be appreciated that a closed group of nodes is established having a security field in which the first component is derived from the network administrator and the second component is derived through at least one of the nodes. This enhances the security of the system because unauthorised access cannot be obtained from information available from the network alone.

In the technique of the invention, the signals are transmitted in blocks, which expression is used to generically denote signal packets, frames, channels etc. It is preferable, although not essential, that the security field be located at the start of each block.

The invention will now be further described with reference to the accompanying drawings, in which:

FIGURE 1 is a schematic illustration of a switched communications network;

FIGURE 2 is a schematic illustration of a QPSX network;

FIGURE 3 is a diagram of part of the network of Figure 2;

FIGURES 4A to E show diagramatically typical signal formats;

FIGURE 5 is a block diagram showing essential steps of the technique of the invention; and

FIGURES 6A to D illustrate a more detailed flow chart of the steps of the invention.

Figure 1 is a schematic illustration of a switched communications network 2 having a plurality of nodes 4 attached thereto. The arrangement includes a Network Administration node 6. The Network Administrator node is generally responsible for administration of the network and performs such tasks as allocating addresses, charging, customer control etc. In the system of the invention, the Network Administrator is also partially involved in the initialization and administration of the security scheme, as will be described hereinafter.

Figure 2 shows a packet switched multi-access network 8 of the type disclosed in International Publication No. WO 86/03639, hereinafter referred to as a "QPSX" network. The QPSX network 8 can be considered as a more specific example of a network upon which the system of the invention can operate. The QPSX network 8 includes oppositely directed unidirectional buses 12 and 14 between which is connected a plurality of access units 10. Each of the access units 10 can be considered as a node in the schematic arrangement illustrated in Figure 1. The access units 10 provide access to users 16, as diagramatically illustrated in Figure 3. The user 16 uses the associated access unit 10 in order to receive and transmit data on the

buses 12 and 14. Broadly speaking, each access unit 10 includes signal processing circuitry which accepts data from the user 16, forms the data into data packets and transmits the packets on the QPSX network 8 in order to reach the access unit associated with the destination node. The access security system of the invention may be implemented by software or hardwired logic at each of the access units 10.

One arrangement for implementation of the system of the invention is to arrange for the access units to form the data into data packets 18, of the type diagramatically illustrated in Figure 4A. In this format, the packet includes an address field 20, security field 22, and data field 17. The address field 20 would normally include the destination network access point (NAP) address and the security field 22 would normally include security information hereinafter referred to as a "VPN Identifier" (Virtual Private Network). The remainder of the packet, the data field 17, would include the message data. In the system of the invention, each node checks the VPN Identifier received by it at least at the beginning of a communication with a node against a list of VPN Identifiers pre-programmed into the node, and, only if a match is found, is the communication accepted. Thus those nodes pre-programmed with a particular VPN Identifier form the closed user group, or Virtual Private Network, associated with that VPN Identifier.

These steps are diagramatically illustrated in the flow chart of Figure 5. The block 24 indicates that the node is waiting receipt of a

message. The block 26 indicates that a message has been received from the network. The block 28 indicates extraction of the VPN Identifier from the message. In block 30, the VPN Identifier is checked to see whether it is the same as that which is stored in the node where the message is received. If yes, the nodes accepts the message, as indicated by block 32. If there is a mismatch, the node discards the message as indicated by block 34 and returns to the wait block 24. These logical steps are carried out by software in microcomputers at the nodes or in hard wired logic implemented to perform the same logical operations.

In accordance with the invention, the VPN Identifier is composed of two or more parts. The first part, referred to here as the "Virtual Private Network Number" (VPN Number), is allocated by the Network Administrator 6, which ensures that the VPN Number is both of a standard format and is unique within that subset of the communications network over which the security scheme extends. Because the Network Administrator 6 ensures that the VPN Number is unique, the entire VPN Identifier is hence unique. The remainder of the VPN Identifier, referred to herein as the "Virtual Private Network Key" (VPN Key), is provided by one or more of the nodes 4 in the closed user group defined by the particular VPN Identifier. These nodes are referred to as the "Master Nodes" of a particular closed user group (of which there may be one or more), as opposed to the "Member Nodes" of the closed user group (of which there may be zero or more). The nodes in the group agree that Master Nodes have the power to

provide VPN Keys, and therefore the power to set up closed user groups. Each Master Node provides a single VPN Key, of a particular format agreed upon by all nodes in the closed user group. This arrangement ensures the uniqueness of the VPN Identifier and ensures that the integrity of the scheme is not predicated upon the integrity of any one party. The VPN Number may comprise a multi-bit digital number randomly generated by the Network Administrator 6. For instance a 16-bit number would be quite suitable. The VPN Key may also comprise a sixteen-bit number which is selected by the user at the node by keyboard or the like or alternatively is automatically generated by an access unit 10 when the user at the access unit requires a new VPN Key.

When it is desired to set up a closed user group or admit another node to an existing closed user group, it is necessary to program the VPN Identifier into the nodes which form the closed user group. This is preferably carried out in a manner which protects the integrity of the VPN Identifier. One technique for setting up the closed user group or admitting another node to an existing closed unit group will now be described with reference to the flow chart which is shown in Figures 6A to D.

Generally speaking, a closed user group is initiated by the Master Nodes requesting a VPN Number from the Network Administrator 6. The latter allocates an available VPN Number to the prospective closed user group, by programming the Master Nodes with the VPN Number. The VPN Number need not necessarily be known to any party other than the

Network Administrator. Users, via Master Nodes then program their own nodes with the associated VPN Keys. A particular VPN Key need not necessarily be known to any party other than the particular the user at a Master Node associated with that key.

The user at a node (either Master or Member) is then admitted in to the closed user group through a multi-party rendezvous at the Member's node, to program the node with the complete VPN Identifier. One example of the procedure for the multi-party rendezvous is described with reference to Figures 6A to D. The Network Administrator supplies the VPN Number and each Master Node supplies the corresponding VPN Key. The node being programmed permits the programming of the node with the appropriate fields (and supplies the appropriate Key if the node is also a Master Node). Typically, the communications with the node being programmed will occur over the network. Alternatively some communications with the node may be made by routes not including the network (out of band) for higher security.

In each case where a node must be programmed with either a VPN Number or Key, the particular field containing the VPN Number or Key may be associated with a "Field Origin Verifier" (FOV), which is a password distributed beforehand by the originator of the particular VPN Number or VPN Key to the node being programmed. Where the communication is out of band, the FOV can be conveyed to a node by secure courier or by other means. The data block carrying the particular VPN Number or Key will also carry the

corresponding FOV and this will be checked at the node being programmed against the Field Origin Verifier entered at the node from the out of band source. Only if these match will the VPN Number or Key be accepted thus precluding an unauthorized node from mimicking a Master Node or the Network Administrator. It will be noted that the integrity of the security scheme is dependent upon the integrity of the FOV's and hence these should be distributed in a secure manner.

Referring now to Figure 6A, the initialization step 36 indicates that a user at a node wants to establish or join a VPN group. The program passes to step 38 which enquires whether or not the node is a Master Node. If the Node is a Master Node, a VPN Key is selected or generated, as indicated by step 40. The program then waits for a received message, as indicated by step 42. If the node is not a Master Node, the program bypasses step 40 and passes directly to Wait Step 42. Once a message has been received at the node, the program determines, in step 44 whether the message has been received either from the network or out of band, for instance an FOV by secure courier. The program then passes to step 46 which determines whether or not the message which has been received contains an FOV for a component of the VPN Identifier. If the message does contain an FOV, the program passes to step 48 shown in Figure 6B.

Step 48 determines whether or not the VPN Identifier component has already been programmed by virtue of an earlier message. If yes, the received

FOV is discarded, as indicated by step 50 and the program returns to Wait Step 42. If the VPN Identifier component has not already been programmed, the program passes to step 52 which determines whether or not the corresponding component of the VPN Identifier i.e. the VPN Number or VPN Key, has already been received from messages from the network. If no, the program stores the FOV, as indicated by step 54 and then returns to a Wait Step 42. If the corresponding component has been received, the program passes to step 56.

In step 56, the program determines whether or not the FOV received from the Network is the same as that which has been received out of band. If the FOV received from the network is different, the program discards all stored fields i.e. any stored values for the VPN Number or VPN Key, as indicated by step 58 and then returns to Wait Step 42. If on the other hand the FOV's match, the program passes to step 60 which stores the received VPN Number from the Network Administrator or the received VPN Key from a Master Node. The program also stores a Field Modification Identifier (FMI) which a password associated with either the VPN Number or VPN Key. The FMI password enables authorized changes of the VPN Number or VPN Key to be made but only if there is a match of FMI's, as described hereinafter. The program then passes to step 62 which determines whether all of the components of the VPN Identifier have been received. In the illustrated arrangement, when the VPN Key and VPN Number have both been received, the programming of the node is complete, as indicated by step 64 from which the program returns

to Wait Step 42. The programmed node is then able to wait for receipt of messages having the correctly encoded VPN Identifiers, as indicated by the operating flow chart of Figure 5. If on the other hand the step 62 indicates that the VPN Number or Key has not yet been received, the program returns to Wait Step 42 to await further messages containing the necessary information.

Returning to Figure 6A, if the step 46 indicates that the message received does not contain an FOV, the program passes to step 66. In this step, the program determines whether the received message contains a component of the VPN Identifier, i.e. the VPN Number or VPN Key and the associated FOV and FMI. If yes, the program passes to step 68, shown in Figure 6B.

The step 68 determines whether or not the received VPN Number or VPN Key has already been stored (in step 60) in respect of an earlier received message. If yes, the program discards the newly received VPN Identifier component, as indicated by step 70 and then returns to Wait Step 42. If there has not been an earlier storing of the VPN Identifier component, the program passes to step 72 which determines whether or not the FOV for the corresponding VPN Identifier component has been received out of band. If yes, the program then passes to step 56 to complete the programming as before. If the corresponding FOV has not been received out of band, the program stores the received VPN Identifier component, FOV and FMI, as indicated in step 74 and then returns to Wait Step 42. The

step 72 thus holds up programming of the node until the FOV has been received from the out of band source.

Returning again to Figure 6A, if the step 66 yields a negative answer, the program passes to step 76. The step 76 enquires whether or not the message includes a request for a VPN Key. If yes, the program passes to step 75 shown in Figure 6C.

The step 75 determines whether or not the node is a Master Node. If it is not a Master Node, it cannot supply a VPN Key and therefore the program returns to Wait Step 42. If yes, the program generates an FOV and FMI, as indicated by step 78. The step 80 indicates the step of conveying the FOV out of band to the requesting node, for instance by secure courier. The program can then send the VPN Key and its associated FOV and FMI to the requesting node via the network, as indicted by step 90. The program then returns to Wait Step 42.

Returning once again to Figure 6A, if the step 76 yields a negative answer, program passes to step 92 which determines whether or not the message contains a modification for a component for the VPN Identifier and the associated FMI (indicated by a message type, for instance), which is transmitted when it is desired to change one or other VPN Identifier components. If the message is not of this type the program returns to Wait Step 42. If the received message does contain a modification to a VPN Identifier component the program passes to step 94 shown in Figure 6D.

The step 94 determines whether or not the corresponding component of the VPN Identifier (to the received FMI) has been stored. If it has not, the program discards the message, as indicated by step 96 and returns to Wait Step 42. If on the other hand the corresponding component of the VPN Identifier has been stored, the program then passes to step 98 which determines whether the received FMI matches with that which has been stored in the node, indicating that the proposed change of the VPN Identifier component is authorized. If there is a mismatch, the signal is discarded, as indicated by step 100 and the program again returns to Wait Step 42. If there is a match of FMI's the program passes to step 102 which stores the modified VPN Identifier component in the node. The received message, in addition to the modified component of the VPN Identifier, may also include a new FMI. The use of new FMI's decreases the likelihood that unauthorized modifications of VPN Identifier components can take place. If a new FMI has been included, it is stored in the node, as indicated by step 104. Thus by the sequence of steps shown in Figure 6D, one or other of the VPN Identifier components can be altered. The program then returns to Wait Step 42 to await receipt of further messages from the network. It is possible of course to have more than two VPN Keys, in addition to the VPN Number.

Figures 4A to E illustrate typical packet formats for signals transmitted in the networks of Figures 1 and 2. The packet format 18 shown in Figure 4A is appropriate for transmission of data between nodes in the network once the VPN groups have

been established. The VPN Identifier field 22 includes separate fields for the VPN Number and for VPN Key_1 to VPN Key_N, which is appropriate for a closed user group with N Master Nodes.

The packet formats 19 and 21 are appropriate when there is a request by a node to form or join a closed user group. The packet format 19 is typical of a packet which is sent by the Network Administrator 6 to a requesting node in order that the requesting node can complete its VPN Identifier. The packet 19 includes the destination NAP Address field 20, FOV field 23, which, as indicated previously, must be matched with the FOV conveyed to the requesting node out of band. It also includes a VPN Number field 25 which contains the VPN Number generated by the Network Administrator 6. Typically the VPN Number could comprise a randomly generated 16-bit number. The signal format also includes an FMI field 27 which is the password enabling subsequent authorized modification of the VPN Number in the field 25.

The packet format 21 shown in Figure 4B is appropriate for the signal sent by a Master Node when requesting to join or form a closed user group. The packet format 21 includes the address field 20, and an FOV field 23, which must match with that of the packet format of Figure 4B in order to establish or join the closed user group. The packet format includes a VPN Key field 29 which contains a coded number generated by the requesting node and which forms the other component of the VPN Identifier for the group. It also includes an FMI field 31 to

enable subsequent authorized modification of the VPN Key 29.

The packet formats 33 and 35 shown in Figures 4D and 4E are appropriate for sending by the Network Administrator and Master Node respectively when it is desired to modify the VPN-Identifier components.

The packet format 33 of Figure 4D includes the address field 20, and a field 37 which contains the old FMI. The password stored in the field 37 must match with the FMI which has been stored in the nodes, in order for new VPN Numbers to be entered. The packet format 33 also includes a field 39 which contains the new VPN Number and a field 41 which contains a new FMI password for subsequent variations of the VPN Number.

The packet format 35 shown in Figure 4E includes the address field 20 and a field 43 which contains the old FMI password which must be matched in order for the VPN Key to be changed. The packet format also includes a field 45 which includes the new VPN Key and a field 47 which includes the new FMI. Since VPN Identifier components are generated independently at separate nodes, there is only a small probability, in general, that the corresponding FMI, are equal since the FMI generation processes will in general be independent.

It will be appreciated that the system of the invention has good security characteristics because access to closed groups of users requires

security components from both the Network Administrator and the nodes. This makes the security system less vulnerable to unauthorised access, since the integrity of the system is not predicated upon the integrity of any single party.

Many modifications will be apparent to those skilled in the art.

CLAIMS:

1. A method of securely transmitting switched signals between nodes (4) which are attached to a communications network (2), said communications network including a network administrator (6), said method including the steps of transmitting signals in blocks (18) at least some of which include security fields (22), checking the security fields at the nodes and accepting the received signal at a node only if first and second components (VPN Number, VPN Key) of the security field have a particular characteristic, and wherein the security field is established by generating the first component (VPN Number) of the security field by the network administrator and generating the second component (VPN Key) of the security field by at least one of the nodes.

2. A method as claimed in claim 1 including the step of establishing a closed group of said nodes each having stored therein a virtual private network (VPN) identifier having first and second components, the first components of the identifiers being unique to said closed group.

3. A method as claimed in claim 2 wherein said particular characteristic is correspondence of the security field received at a node with the VPN identifier programmed into that node.

4. A method as claimed in claim 2 or 3 wherein the signals are transmitted in packets (18) and wherein each packet includes a destination address

field (20), security field (22) and data field (17).

5. A method as claimed in claim 4 wherein the security access field includes a VPN Number field generated by the network administrator and a plurality VPN Key fields each associated with a master node in the group, the master nodes each being capable of providing VPN Keys, the other nodes not being capable.

6. A method as claimed in claim 5, wherein the method of establishing the closed user group includes the step of the master nodes of the closed user group requesting a VPN Number from the network administrator and themselves generating their respective fields of the VPN Key.

7. A method as claimed in claim 6 wherein a node requesting to join the closed user group, either during the initialization of the closed user group or to join an already existing closed user group, joins the closed user group through a multi-party rendezvous, wherein the network administrator supplies the requesting node with the VPN Number and the master nodes of the closed user group supply the requesting node with with the VPN Key fields, other than the VPN Key field which is supplied by the requesting node itself, in the case where the requesting node is also a master node of the closed user group.

8. A method as claimed in claim 7 including the step of transmitting from the network administrator to said requesting node a packet which includes a

field origin verifier (FOV) field and a VPN Number field and wherein the VPN Number field contains the said first component of the VPN Identifier.

9. A method as claimed in claim 8 including the step of transmitting from each of the master nodes in the closed user group, with the exception of the requesting node, in the case that the requesting node is itself a master node, to said requesting node packets which includes a field origin verifier (FOV) field and a VPN Key field and wherein the VPN Key field contains the said second component of the VPN Identifier.

10. A method as claimed in claim 9 including the step of transmitting to the requesting node a password which corresponds to the FOV transmitted with the relevant component of the VPN Identifier and wherein the password is not transmitted to the requesting node via the network.

11. A method as claimed in claim 10 including the step of storing said first and second components of the VPN Identifier in the requesting node only if there is correspondence between the contents of the FOVs transmitted with the components of the VPN Identifier and the respective passwords.

12. A method as claimed in claim 11, wherein the case that the requesting node is a master node of the closed user group, the requesting node generates and stores a VPN Key.

13. A method as claimed in claim 12, wherein

said packets which include FOVs also include Field Modification Indentifiers (FMI) fields and if there is correspondence between a third component of the security field stored at a node and the content of the FMI field, a change to the first and/or second component of the VPN Identifier field is permitted.

14. A method as claimed in claim 13 including the step of the transmitting from a master node or the network administrator to nodes in the closed user group a packet which includes a current FMI field, a new VPN Key field or VPN Number, respectively, and a new FMI field and permitting subsequent modifications of the VPN Identifier component only if there is correspondence between the third component and the content of the new field modification field.

15. A security system for a switched communications network (2), which includes a network administrator (6), and to which is attached a plurality of nodes (4), said system comprising means (10) for transmitting signals between said nodes in signal blocks (18) at least some of which include security fields (22), checking means at the nodes for checking the security fields to determine whether or not first and second components (VPN Number, VPN Key) thereof have particular characteristics, and wherein said network administrator includes means for generating the first component of the security field (VPN Number) and at least one of said nodes includes means for generating a second component (VPN Key) of the security field.

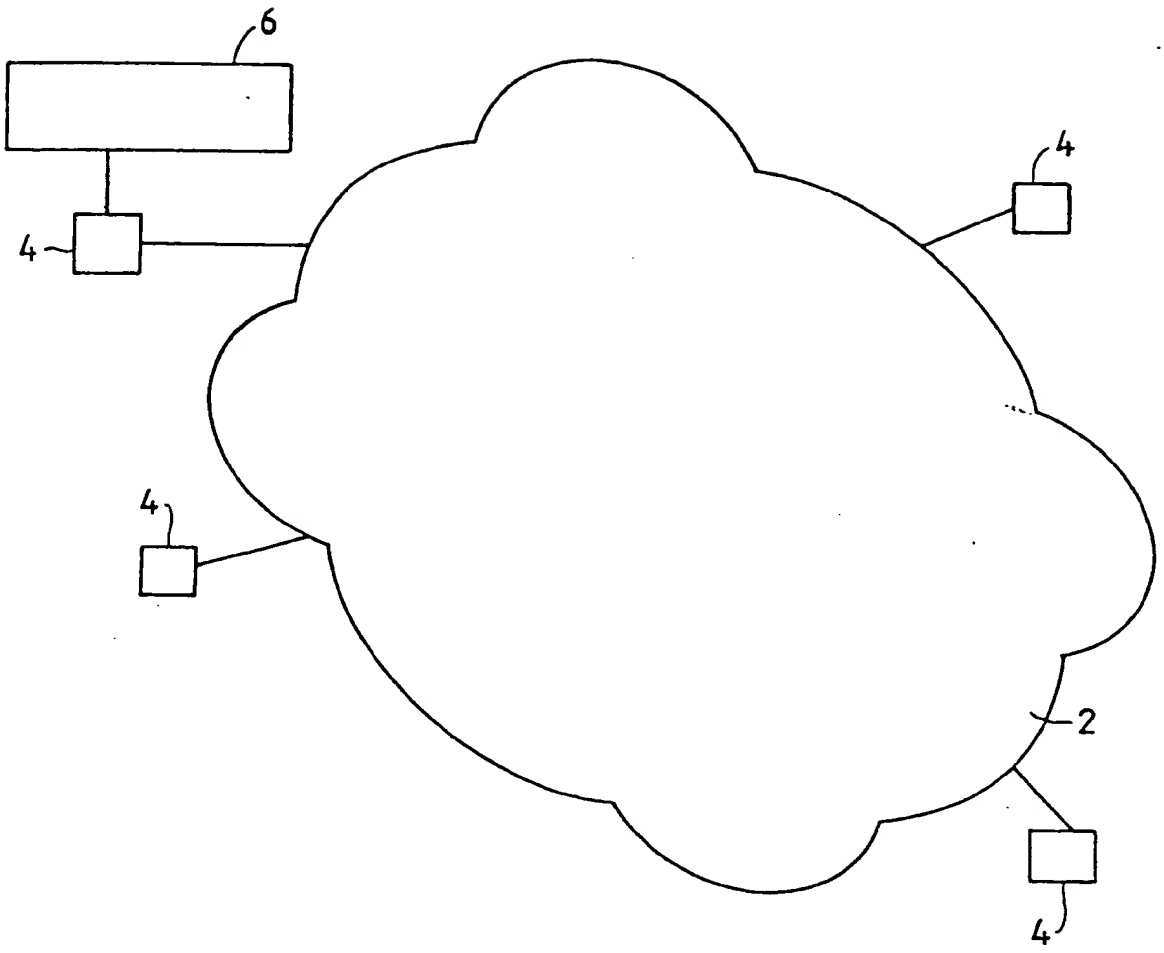


FIG 1

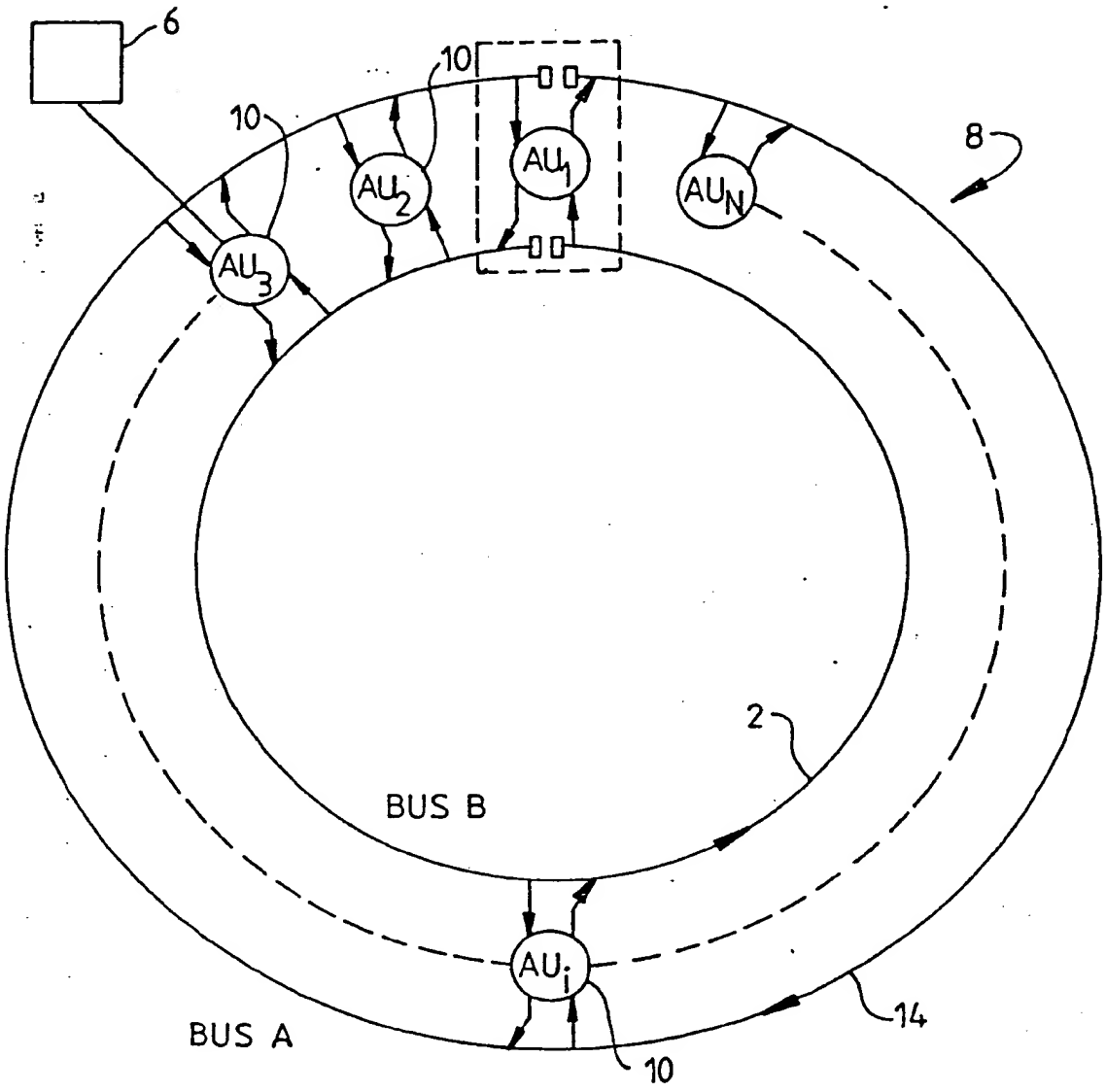


FIG 2

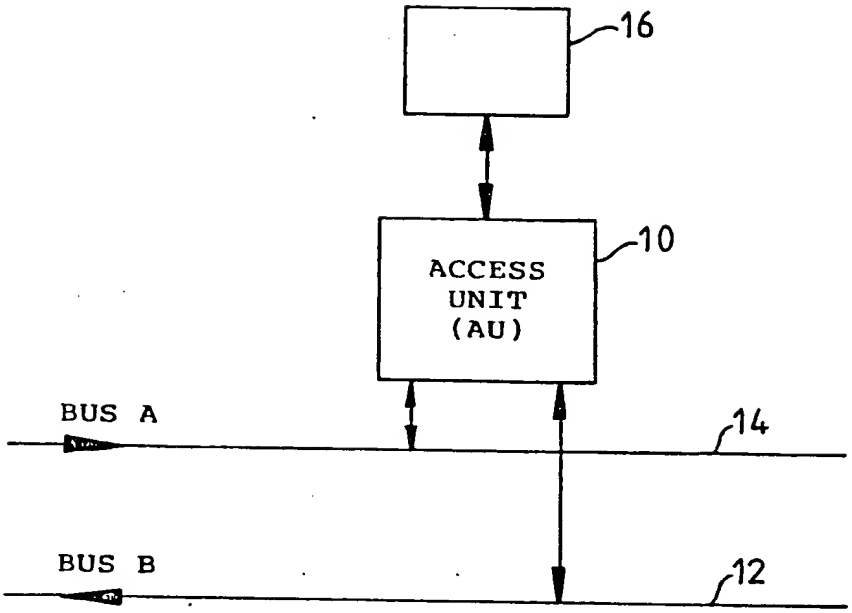


FIG 3

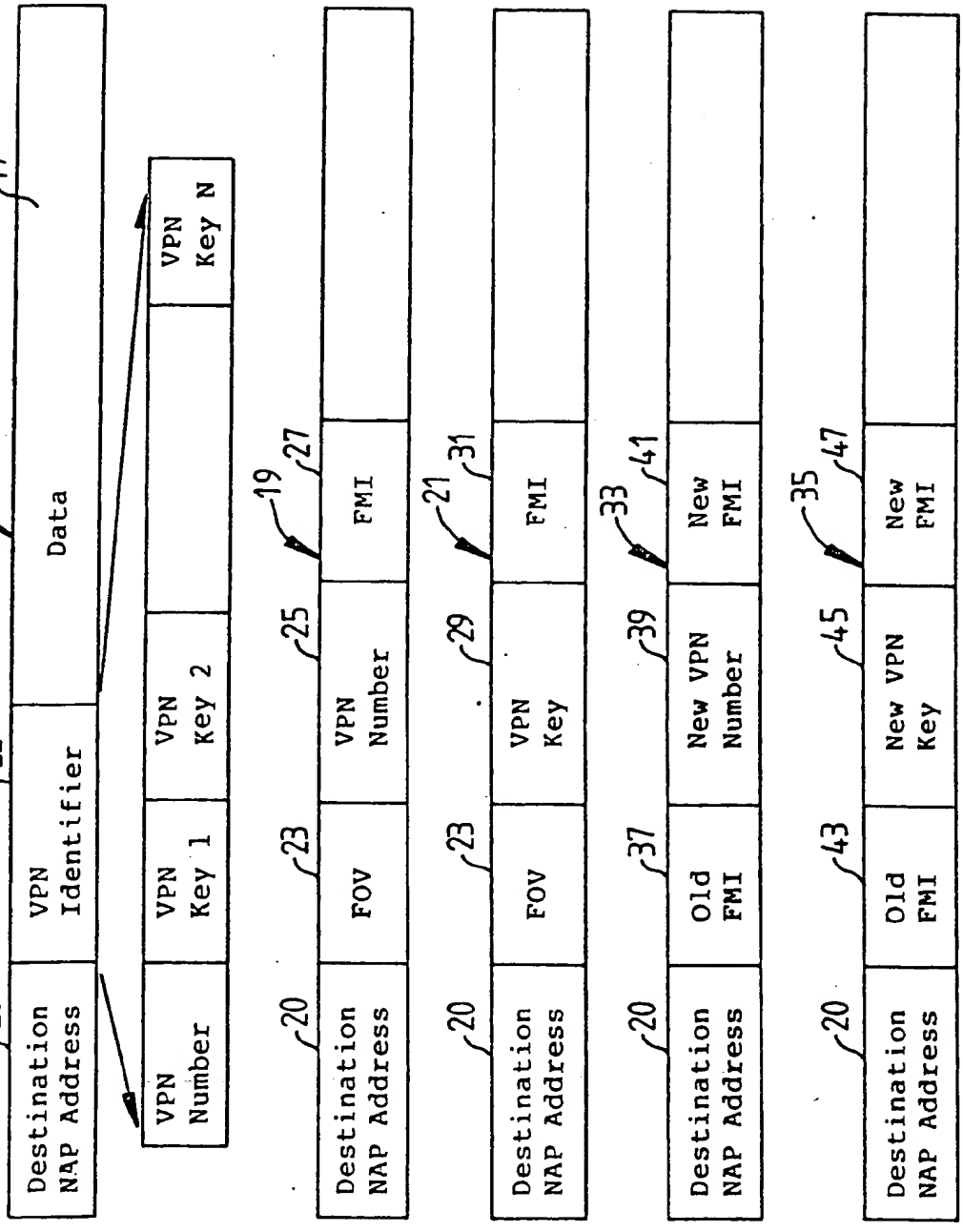


FIG 4A

FIG 4B

FIG 4C

FIG 4D

FIG 4E

SUBSTITUTE SHEET

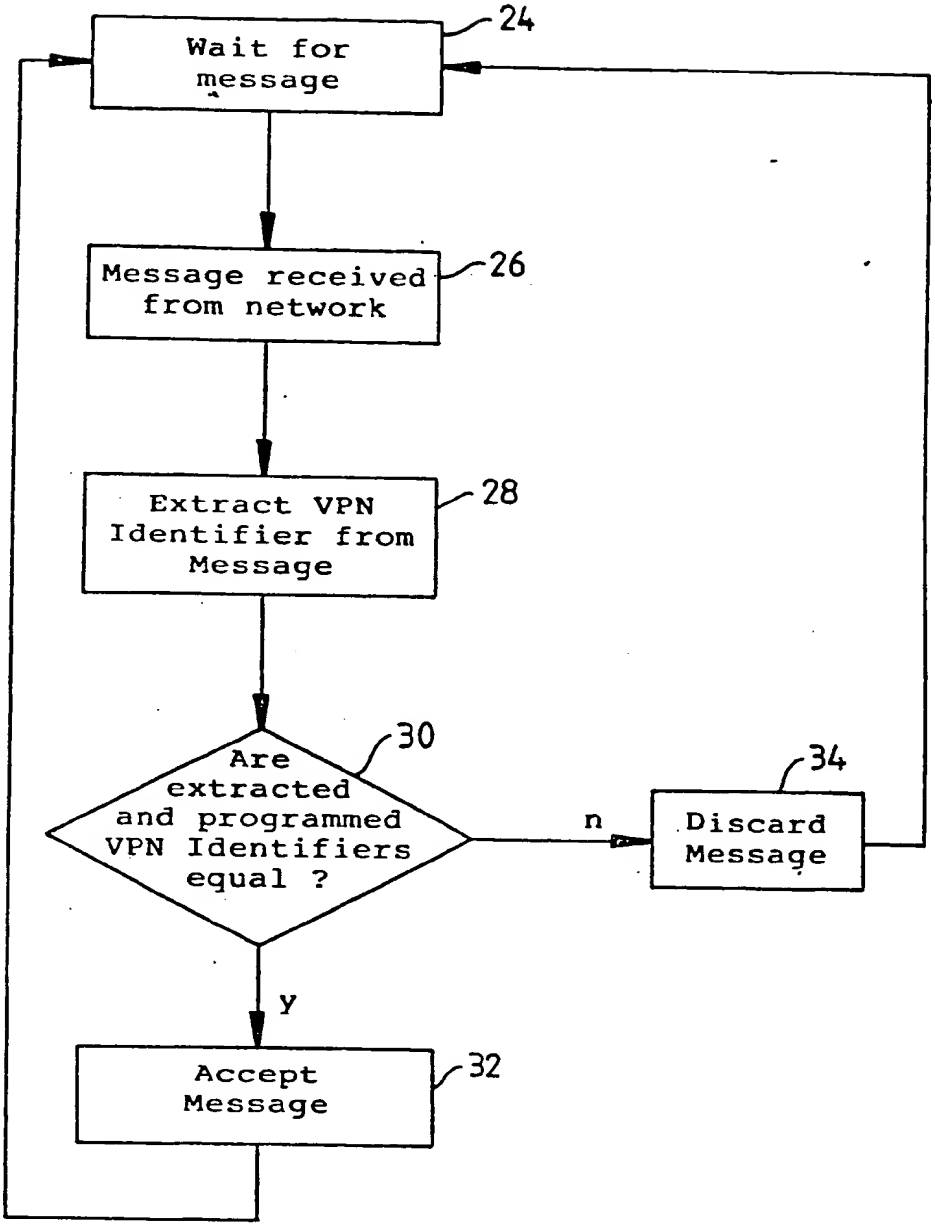


FIG 5

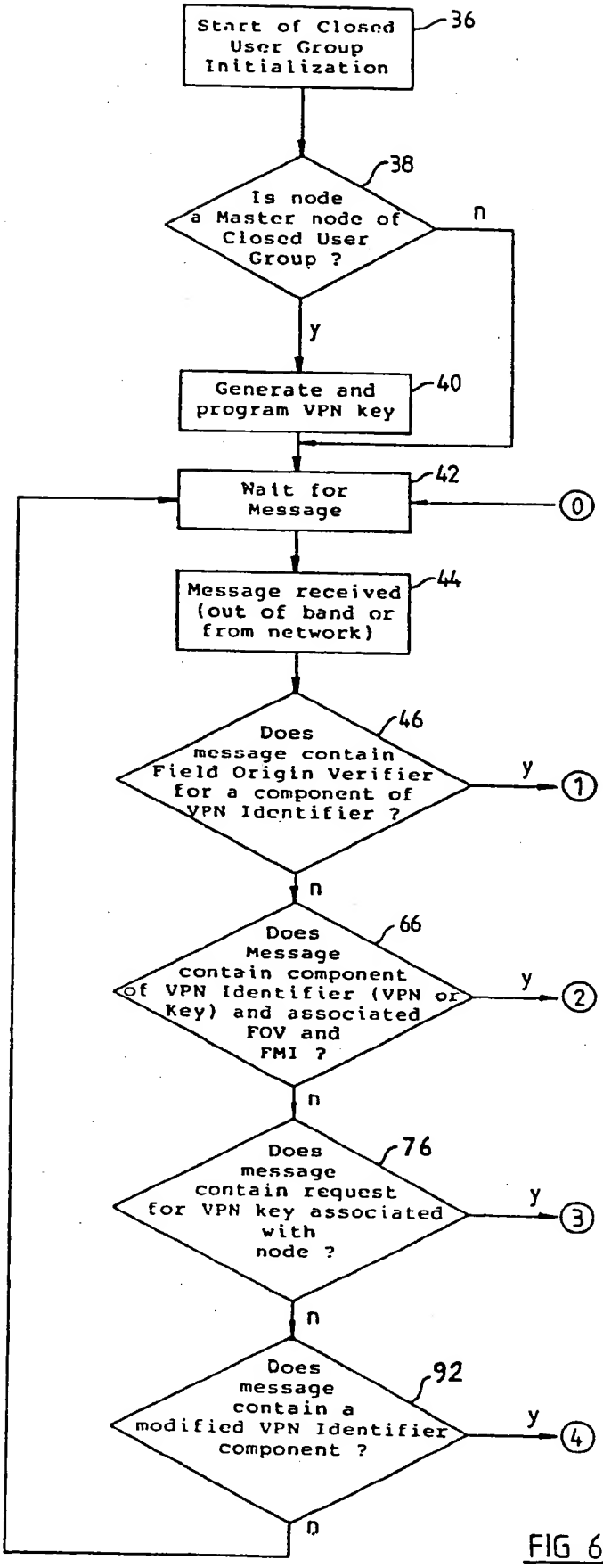


FIG 6A

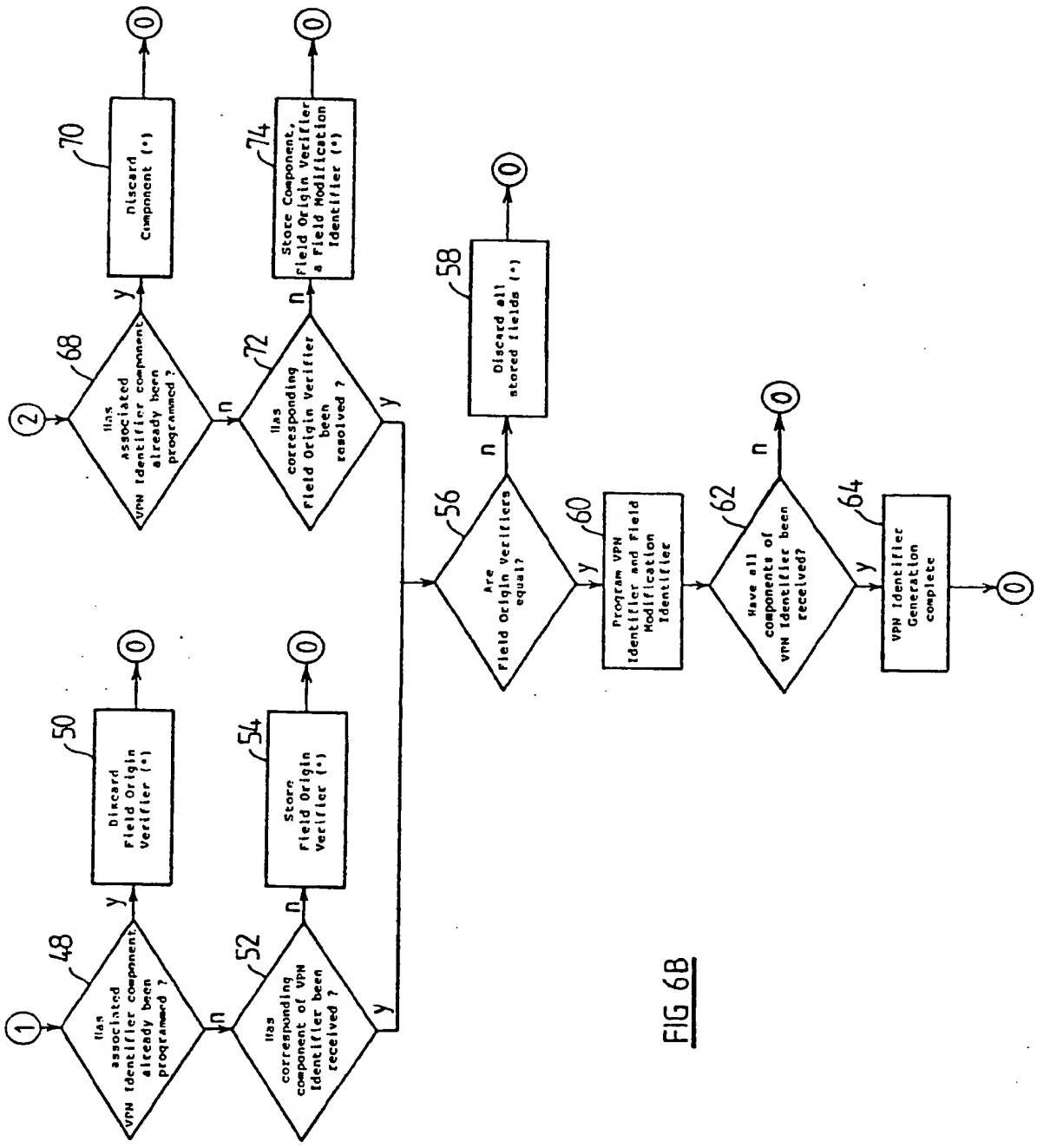

1
2
Has associated VPN Identifier component already been programmed ?
48
y
n
Discard Field Origin Verifier (*)
50
Has corresponding component of VPN Identifier been received ?
52
Store Field Origin Verifier (*)
54
Are Field Origin Verifiers equal?
56
Discard all stored fields (*)
58
Program VPN Identifier and Field Modification Identifier
60
Have all components of VPN Identifier been received?
62
VPN Identifier Generation complete
64
Has associated VPN Identifier component already been programmed ?
68
Discard Component (*)
70
Has corresponding Field Origin Verifier been resolved ?
72
Store Component, Field Origin Verifier & Field Modification Identifier (*)
74
0

FIG 6B

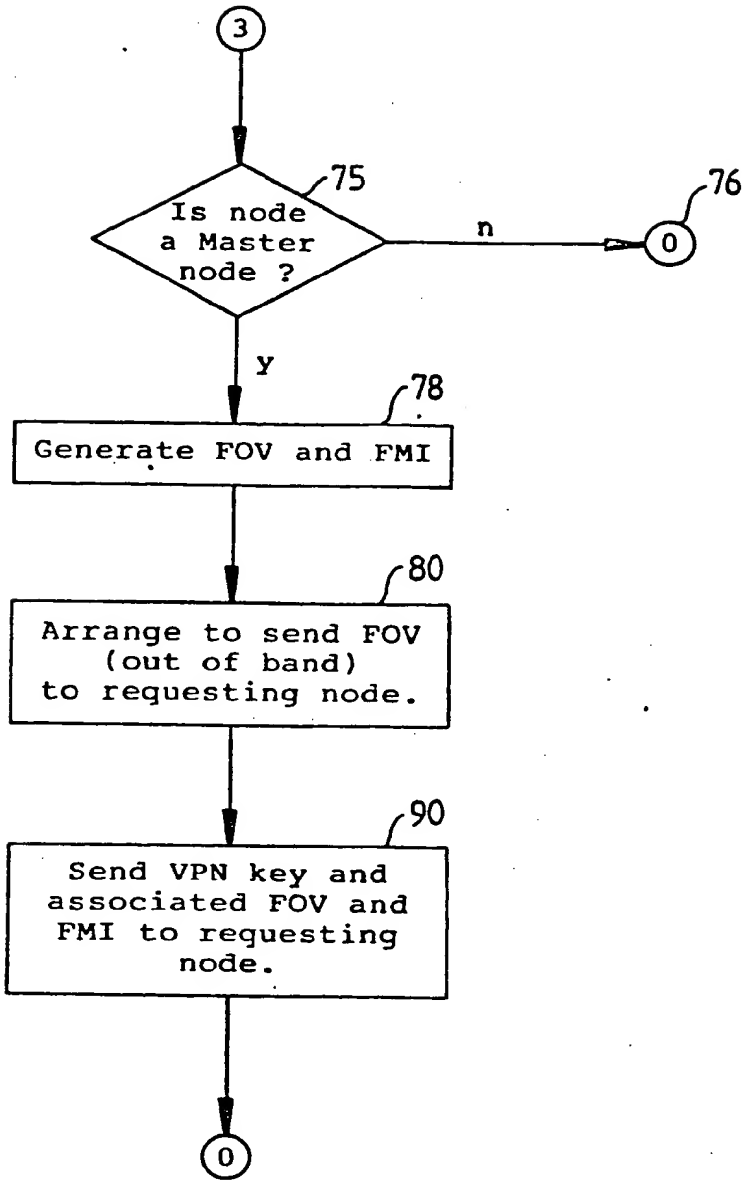

3
75
Is node a Master node ?
n
76
0
y
78
Generate FOV and FMI
80
Arrange to send FOV (out of band) to requesting node.
90
Send VPN key and associated FOV and FMI to requesting node.
0

FIG 6C

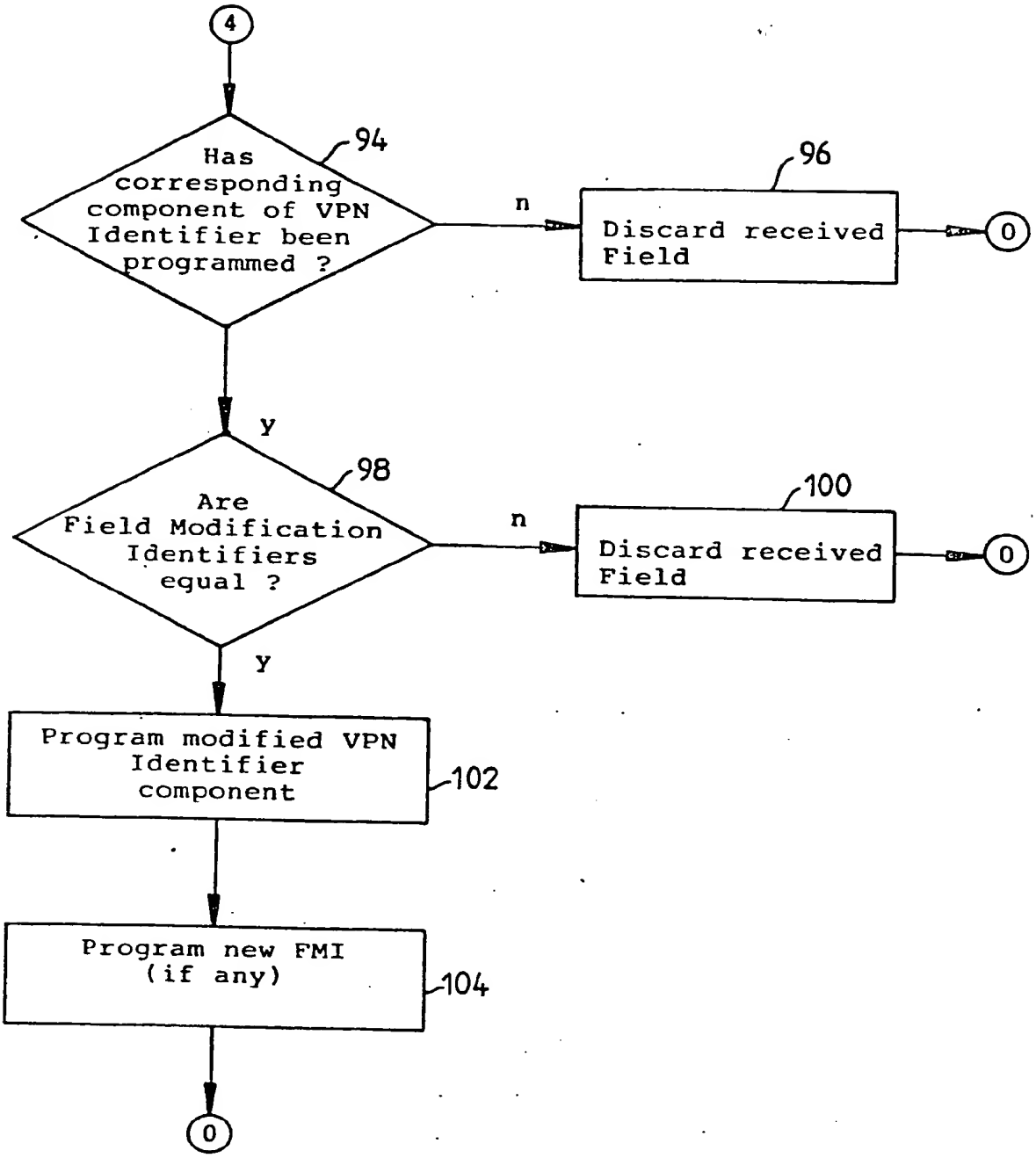

4
Has corresponding component of VPN Identifier been programmed ?
94
n
Discard received Field
96
0
y
Are Field Modification Identifiers equal ?
98
n
Discard received Field
100
0
y
Program modified VPN Identifier component
102
Program new FMI (if any)
104
0

FIG 6D

INTERNATIONAL SEARCH REPORT

International Application No PCT/AU 89/00098

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

Int. Cl.[4] G06F 13/14, 13/38; H04L 9/00, 11/26

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
IPC	G06F 13/14, 13/38; H04L 9/00, 11/26

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [8]

AU : IPC as above

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category [10]	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
P,A	Patents Abstracts of Japan, E-699, page 165 JP,A, 63-212261 (BITSUGU SONS K.K.) 27 December 1988 (27.12.88)	
P,A	AU,A, 78322/87 (WANG LABORATORIES, INC.) 23 June 1988 (23.06.88)	
A	Patents Abstracts of Japan, P-667, page 67 JP,A, 62-197850 (MITSUBISHI ELECTRIC CORP.) 16 February 1988 (16.02.88)	
A	AU,A, 76214/87 (HONEYWELL BULL INC.) 4 February 1988 (04.02.88)	
A	AU,A, 76189/87 (AMERICAN TELEPHONE AND TELEGRAPH COMPANY) 4 February 1988 (04.02.88)	
A	EP,A2, 0223122 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 27 May 1987 (27.05.87)	
A	AU,A, 57948/86 (SIEMENS AKTIENGESELLSCHAFT) 4 December 1986 (04.12.86)	
A	AU,A, 24126/84 (559620) (TRW, INC.) 2 August 1984 (02.08.84)	

(continued)

* Special categories of cited documents: [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
8 June 1989 (08.06.89)	20 June 1989 (20.06.89)
International Searching Authority	**Signature of Authorized Officer**
Australian Patent Office	A J Evans A.J. EVANS

Form PCT/ISA/210 (second sheet) (January 1985)

FURTHER INFORMATION CONTINUED FROM THE SECOND SHEET

A	AU,A, 21957/83 (566427) (INTERNATIONAL STANDARD ELECTRIC CORPORATION) 28 June 1984 (28.06.84)	
A	AU,A, 89379/82 (553726) (NATIONAL RESEARCH DEVELOPMENT CORPORATION) 21 April 1983 (21.04.83)	
A	EP,A1, 0048903 (LICENTIA PATENT-VERWALTUNGS-GmbH) 7 April 1982 (07.04.82)	

V ☐ OBSERVATIONS WHERE CERTAIN CLAIMS WERE FOUND UNSEARCHABLE [1]

This international search report has not been established in respect of certain claims under Article 17(2) (a) for the following reasons:

1. ☐ Claim numbers ..... because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claim numbers ..... because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claim numbers ..... because they are dependent claims and are not drafted in accordance with the second and third sentences of PCT Rule 6.4(a).

VI ☐ OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING [2]

This International Searching Authority found multiple inventions in this international application as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims of the international application.

2. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims of the international application for which fees were paid, specifically claims:

3. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claim numbers:

4. ☐ As all searchable claims could be searched without effort justifying an additional fee, the International Searching Authority did not invite payment of any additional fee.

Remark on Protest

☐ The additional search fees were accompanied by applicant's protest.

☐ No protest accompanied the payment of additional search fees.